AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☑ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* information associated with email address cashaythickgirl@yahoo.com and telephone number 414-349-5994 (the "accounts") stored at Apple, Inc. (See Attachments)	Case No. 23-966M(NJ) **Matter No.: 2023R00086**

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin *(identify the person or describe the property to be searched and give its location)*:

See Attachment A. Over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before August 7, 2023 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph .
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 7/24/2023 @ 1:24 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email address cashaythickgirl@yahoo.com and telephone number 414-349-5994 (the "accounts") that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple, Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple, Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) from January 1, 2021 to the present, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the accounts were created, the length of service, the IP address used to register the accounts, account status, associated devices, methods of connecting, and means and source of payments (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Number ("MEIN"), Mobile Equipment Identifiers

("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identifies ("IMEI");

c. The contents of all instant messages associated with the accounts from January 1, 2021, to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message.

d. The contents of all emails associated with the accounts from January 1, 2021, to present, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks,

and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violation of 18 U.S.C. § 249 involving Cordell M. Howze and C.H. and occurring after January 1, 2021, including, for each account identifier listed on Attachment A, information pertaining to the following matters:

(a) Any information related to possession of firearms (including photographs, text messages, emails, or any other communication information);

(b) Any information regarding biases or hate regarding sexual orientation;

(c) Any information recording the target's schedule or travel between January 1, 2021 to present;

(d) Any web search information related to the offenses described above;

(e) Any communications via text message, email, Facebook, Twitter, SnapChat, or other web-based applications between the subject and others regarding the offenses described above;

(f) Any photographs or videos regarding the offenses described above; and

(g) All bank records, checks, credit card bills, account information, and other financial records.

(h) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(i) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(j) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with email address cashaythickgirl@yahoo.com and telephone number 414-349-5994 (the "accounts") stored at Apple, Inc. (See Attachments)

Case No. 23-966M(NJ)

Matter No.: 2023R00086

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A. Over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 249	Hate Crime Acts;

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Erin Lucker, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 7/24/2023

Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Erin Lucker, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703 (c)(I)(A) to require Apple Inc. (hereinafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with an Apple ID that is stored at its premises owned, maintained, controlled or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent for the Federal Bureau of Investigation ("FBI"), where I have been employed since November 2016. I am currently assigned to an FBI squad which investigates civil rights crimes and public corruption crimes. I was previously assigned to the FBI Milwaukee Violent Crimes Task Force which involved investigations of violent crimes, to include kidnappings, extortions, murder for hire, and bank and armored car robberies. During my tenure with the FBI, I have participated in all aspects of investigations, including executing search warrants involving, among other things, the search and seizure of computers, computer equipment, software, and electronically stored information. Through my experience and training, I have become familiar with activities of individuals engaged in illegal activities, to include their techniques, methods, language, and terms. During my career, my investigations have included the use of various surveillance techniques and the execution of numerous search and seizure warrants, including for computers and cellular telephones.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies, all of whom I believe to be truthful and reliable. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that the information described in Attachment A contains evidence of violations of 18 U.S.C. § 249, as described in Attachment B.

JURISDICTION

5. This court has jurisdiction to issue the requested warrant because it is a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§2703(a), (b)(I)(A), & (c)(I)(A). Specifically, the Court is "a district court of the United States … that has jurisdiction over the offense being investigated." 18 U.S.C § 2711(3)(A)(i).

PROBABLE CAUSE

6. On Sunday, February 26, 2023, witness G.V. (DOB 9/20/1999) was sleeping at 5301 N. 29th Street, Apartment 7, Milwaukee, Wisconsin and woke up at approximately 5:33 a.m. after hearing a loud bang that could have been a gunshot. Between 8:15 a.m. and 8:30 a.m., G.V. smelled gas in the apartment and checked the stove to ensure there was not a gas leak. At approximately 9:15 a.m., G.V. observed light smoke in the apartment and contacted 911.

7. On Sunday, February 26, 2023, at approximately 9:21 a.m., Milwaukee Fire Department ("MFD") was dispatched to 5301 N. 29th Street, Milwaukee, Wisconsin, regarding a structure fire at that location. Upon arrival, MFD observed that Apartment 5 was on actively on fire and forced entry. After the fire was extinguished and the apartment was vented, MFD discovered a deceased

victim, who was identified as C.H. (DOB 6/14/1991). C.H. was a transgender female who was assigned male at birth.

8. Milwaukee Police Department ("MPD") responded to the scene and conducted a scene investigation. Located in the residence was a red, plastic gas can with gasoline inside. In addition, one (1) 9mm cartridge was recovered in the bathroom of the residence. Also located in the residence was an Apple iPhone, which was placed in evidence at MPD under Inventory # 23006653, Item #12. A red, 2019 Toyota Camry, Wisconsin license plate ARZ2792, registered to C.H., was recovered from the rear parking lot of 5301 N. 29th Street and towed to the City of Milwaukee Tow Lot for evidence processing.

9. A review of surveillance video captured an unidentified male (UM-1) walking south across the rear parking lot of 5277 S. 29th Street, Milwaukee, Wisconsin, at approximately 8:45 a.m. UM-1 continued behind the garage of 5266 N. Teutonia Avenue, Milwaukee, Wisconsin. Pole camera video then captured UM-1 walking on the driveway of 5262 N. Teutonia Avenue, Milwaukee, Wisconsin, and crossing Teutonia Avenue to the west side of the street. Additional pole camera video showed UM-1 walking south to Villard Avenue towards McDonalds, 5191 N. Teutonia Avenue, Milwaukee, Wisconsin, and then continuing to walk south on Teutonia Avenue, out of view of surveillance video and pole cameras.

10. In the surveillance and pole camera videos, UM-1 was observed wearing a black vest with a hood over a gray sweatshirt, light colored sweatpants with a dark colored stripe from the waist to the knees. UM-1 had glasses on top of his head and had his hair braided toward the back with short or shaved hair on the sides.

11. C.H.'s 2019 Toyota Camry was processed for evidence and latent prints were recovered from a Lysol wipes container located on the front passenger floorboard. An examination of the latent prints revealed a match to the left ring finger of CORDELL M. HOWZE (DOB 10/26/1989).

12. MPD officers interviewed P.S. (DOB 12/5/1996), who advised that HOWZE spent the night at P.S.'s home in Neenah, Wisconsin on Friday, February 24, 2023. On Saturday, February 25, 2023, P.S. gave HOWZE a ride to Milwaukee, Wisconsin, and dropped HOWZE off on 83rd Street at approximately 10:30 a.m. At this time, HOWZE was wearing light colored cargo pants and a dark jacket with grey sleeves. P.S. was shown surveillance still images of UM-1 from McDonalds, 5191 N. Teutonia Avenue, Milwaukee, Wisconsin. P.S. advised UM-1 looked like HOWZE, and the clothing UM-1 was wearing was consistent with clothes HOWZE was wearing when P.S. drove HOWZE to Milwaukee, Wisconsin, on Saturday, February 25, 2023.

13. On Monday, February 27, 2023, P.S.'s wife contacted P.S. and advised HOWZE was at their home in Neenah, Wisconsin. P.S. responded to his home and observed HOWZE in the living room with a black, red dot sight handgun with an extended magazine and green laser beam. HOWZE showed P.S. videos on HOWZE'S cell phone, which P.S. identified as HOWZE's white Apple iPhone. In the video, P.S. heard HOWZE'S voice, and in addition, P.S. recognized HOWZE'S face in the reflection of an aquarium. The video showed a deceased female wearing a t-shirt and underwear. There was an injury to the back of the female's head, and there was blood on the floor and pillows. In the video, HOWZE pointed a gun at an aquarium and pointed the green laser beam at a snake in the aquarium. P.S. observed that the video was shot on the second floor of a building. In addition, P.S. observed a yellow house through the window.

14. P.S.'s description of the video, to include the deceased woman, location of the injury, and the aquarium, was consistent with the February 26, 2023 crime scene at 5301 N. 29th Street, Apartment 5, Milwaukee, Wisconsin.

15. HOWZE told P.S. that HOWZE "caught a body of a disgusting ass transgender." HOWZE made comments that he wanted to kill a female that drove a red Dodge Caravan, and a male that kept contacting HOWZE about a vehicle HOWZE stole. At this time, P.S. told HOWZE to leave P.S.'s home. P.S. observed HOWZE had two cell phones; P.S. identified these cell phones as a red Apple iPhone with telephone number 920-205-4720, and a white Apple iPhone with telephone number 414-581-2266. HOWZE sent P.S. the same video via text message from telephone number 414-581-2266. P.S. deleted the video because P.S. was disgusted by the content.

16. On February 28, 2023, HOWZE was observed exiting an apartment building in Neenah, Wisconsin, and entering a 2019 White Chevrolet Trax, Wisconsin license plate AEZ6823, registered to R.H. (DOB 1/12/1968), which is HOWZE's mother. City of Neenah Police Department ("NPD") Officers attempted to conduct a vehicle stop of HOWZE, but HOWZE continued to drive away. During the pursuit, officers observed HOWZE throw items from the Chevrolet Trax, which included a blue Nike duffle bag; a clear, plastic bag containing unfired, 9mm cartridges; a black Sig Sauer P320 9mm semi-automatic handgun, serial number 58B229642, with a green laser attachment; and a white iPhone. After the pursuit, HOWZE was taken into custody in Menasha, Wisconsin. The items thrown from the Chevrolet Trax were collected by law enforcement, including the white iPhone, which was placed in evidence at MPD under Inventory #23006928, Item #1.

17. On March 1, 2023, HOWZE'S mother, R.H., was interviewed by MPD detectives. R.H. advised she gave HOWZE a ride to Dunham's, 2550 S. 108th Street, West Allis, Wisconsin on

Saturday, February 25, 2023, where HOWZE purchased a box of 9mm 100 gr FMJ lead ammunition. R.H. provided detectives with the receipt from Dunham's, which showed the purchase was made on February 25, 2023, at approximately 4:05 p.m. R.H. was aware that HOWZE possessed a handgun with a green laser.

18. R.H. advised she and HOWZE went to an AT&T store on Saturday, February 25, 2023, in order to purchase new iPhones. R.H. identified HOWZE'S new telephone number as 414-581-2266.

19. R.H. was shown surveillance still images of UM-1 from the area of 5301 N. 29th Street, Milwaukee, Wisconsin. R.H. identified UM-1 as being HOWZE and advised the clothing UM-1 wore was consistent with the clothing HOWZE wore when he left R.H.'s home on Saturday, February 25, 2023 and Sunday, February 26, 2023.

20. On March 16, 2023, a search warrant authorizing the forensic examination of the white Apple iPhone (MPD Inventory #23006928, Item #1) was executed. The extraction revealed the device's MSISDN was 414-581-2266 and the Apple ID was cordell.howze@icloud.com.

21. The extraction included the device's web history, which showed the device accessed https://transx.com.listcrawler.eu. Per listcrawler.eu, the website is an escort advertisement list-viewer that displays daily classified advertisements from a variety of sources, to include megapersonals.eu. The escorts advertised in the transx.com.listcrawler.eu section was described as "trans and shemale escorts." The device accessed https://transx.com.listcrawler.eu/post/escorts/usa/wisconsin/milwaukee/116573863 ("Post 116573863).

22. On April 11, 2023, investigators accessed "Post 116573863". The advertisement had a time stamp of "Sat 25 Feb 2023 11:07 PM" and noted the escort was "fully functional." The contact

telephone number for the escort was listed as 414-349-5994. The escort's location was listed as Highway 41 and College Avenue in Milwaukee, Wisconsin. Photographs in the advertisement matched known photographs of C.H. On February 27, 2023, A.G., a friend of C.H., was interviewed by MPD detectives. A.G. identified C.H.'s telephone number as 414-349-5994. According to A.G., C.H. was an escort that posted advertisements on Facebook and megapersonals.eu.

23. The iPhone extraction included a screenshot of a text message from telephone number 414-349-5994, known to be used by C.H. C.H. texted "I'm here", "U on the left or the right side", "?", and "I'm here."

24. The iPhone extraction included videos saved on the device. A one minute and one second video (file name IMG_0011.MOV) depicted a female in a residence, lying on the floor with a blanket partially covering her body and a pillow on her head. The individual taking the video held a firearm with a green laser in their right hand. The individual pointed the laser at the female on the floor. A voice says: "Ya'll wanna see a dead body?" and the blanket is removed from the female. The pillow is moved, revealing a gunshot wound on the female's head. The handgun with the green laser is then pointed at the female's head. A voice says: "This is just the beginning. Prime example, my goofy ass n*****, crossing the line by trying to be somebody he really isn't."

25. A 41 second video (file name IMG_0009.MOV) depicted an individual walking around a residence. The individual walked in to the bathroom, where he was observed in the bathroom mirror. The individual took the magazine out of a handgun and locked the slide back. The individual observed in the mirror matches known photographs of HOWZE.

26. A 10 second video (file name IMG_0010.MOV) depicted a female in a residence, lying on the floor with a blanket partially covering her body and a pillow on her head. The individual taking the video held a firearm with a green laser in their right hand. The individual pointed the laser at the female on the floor.

27. The iPhone extraction included text messages between telephone number 414-581-2266, known to be used by HOWZE, and P.S. On February 27, 2023, at approximately 8:05 p.m., HOWZE texted video IMG_0010.MOV to P.S. On February 28, 2023 at approximately 10:58 a.m. video IMG_0012.MOV was texted from HOWZE to P.S.

28. The iPhone extraction included February 2023 SnapChat messages between usernames snoopallday23 and lovie1674. SnapChat is an Internet-based mobile application that provides a way to share photos, videos and messages. The pictures and videos shared are available to the receiver for a short time before it becomes inaccessible.

29. The extraction of the iPhone revealed the device's MSISDN was 414-581-2266. Both P.S. and R.H. identified HOWZE'S new telephone number as 414-581-2266. In addition, the extraction revealed an iCloud account was present on the device and identified the Apple ID as cordell.howze@icloud.com.

30. MPD conducted a forensic examination of the Apple iPhone recovered from the crime scene (MPD Inventory #23006653, Item #12). The extraction revealed the device's MSISDN was 414-349-5994 and the Apple ID was cashaythickgirl@yahoo.com. Telephone number 414-349-5994 was the listed contact telephone number on escort advertisements that depicted photographs that matched known photographs of C.H. In addition, A.G. identified C.H.'s telephone number as 414-349-5994.

31. On April 13, 2023, a preservation request under 18 U.S.C. § 2703(f) was sent to Apple regarding Apple accounts registered under telephone number 414-349-5994. On June 29, 2023, a preservation request under 18 U.S.C. § 2703(f) was sent to Apple regarding Apple accounts registered under email address cashaythickgirl@yahoo.com.

32. Law enforcement has identified C.H.'s iCloud Account and seeks to search that account for evidence of violations of 18 U.S.C § 249.

33. From my training and experience, I know that iCloud is a cloud storage and cloud computing service that Apple provides to its customers and is accessible on their products, including the iPhone. Customers can use the iCloud to backup information, to include SMS and MMS messages, photos, videos, music, calendars, third-party app data, and purchase history from Apple, that is captured and/or stored on their personal mobile devices.

34. From my training and experience, I know that Apple customers may use iCloud to back-up their mobile devices, including iPhones, iPads, and Macs, as a way to ensure that important information is not lost, as well as a means to save important information that is taking up too much space on their mobile device. It is also a way to ensure that when a mobile device is replaced – either for an upgrade or because a device has been lost, stolen, or damaged, the Apple customer can restore data to the new phone. Relatedly, I understand that items may have been accidentally or intentionally deleted or otherwise unrecoverable from a device may remain in an iCloud account.

35. There is probable cause to believe that evidence of the specified federal offenses will be found in the Target Account because the evidence gathered to date in the investigation suggests that C.H. used an Apple device to record images and videos, and to communicate with individuals in an attempt to meet. Based on my training and experience, I know that individuals involved in

criminal schemes often communicate with others, be it victims, conspirators, or unknowing parties, in furtherance of their activities. Here, there is probable cause to believe C.H. used a cell phone number and other applications, to include SnapChat, to communicate with others, and to transmit messages relating to the specified federal offenses. There is therefore probable cause to believe that the Target Account will provide evidence, including but not limited to, communications between C.H. and HOWZE, as well as photographs, videos, and Internet searches relating to the specified federal offenses.

INFORMATION REGARIDNG APPLIE ID AND iCLOUD[1]

36. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

37. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages")

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

38. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

39. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated

with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

40. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

41. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an

Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

42. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

43. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

44.For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience,

instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

45. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

46. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

47. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity,

documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

48. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

49. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(I)(A) and 2703(c)(I)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

50. Based on the forgoing, I request that the Court issue the proposed search warrant.

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

52. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email address cashaythickgirl@yahoo.com and telephone number 414-349-5994 (the "accounts") that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple, Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple, Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) from January 1, 2021 to the present, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the accounts were created, the length of service, the IP address used to register the accounts, account status, associated devices, methods of connecting, and means and source of payments (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Number ("MEIN"), Mobile Equipment Identifiers

("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identifies ("IMEI");

c. The contents of all instant messages associated with the accounts from January 1, 2021, to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message.

d. The contents of all emails associated with the accounts from January 1, 2021, to present, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks,

and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violation of 18 U.S.C. § 249 involving Cordell M. Howze and C.H. and occurring after January 1, 2021, including, for each account identifier listed on Attachment A, information pertaining to the following matters:

(a) Any information related to possession of firearms (including photographs, text messages, emails, or any other communication information);

(b) Any information regarding biases or hate regarding sexual orientation;

(c) Any information recording the target's schedule or travel between January 1, 2021 to present;

(d) Any web search information related to the offenses described above;

(e) Any communications via text message, email, Facebook, Twitter, SnapChat, or other web-based applications between the subject and others regarding the offenses described above;

(f) Any photographs or videos regarding the offenses described above; and

(g) All bank records, checks, credit card bills, account information, and other financial records.

(h) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(i) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(j) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.